

REMARKS

The Examiner's action and the grounds for rejection set forth therein have been carefully considered. Claims 40-65 remain in the application. Claim 40 is the only independent claim.

Claims 40-41, 45-50 and 54-63 stand rejected under 35 USC 102(e) as being anticipated by Candelore (U.S. Patent Application Publication No. 2003/0081776). Claims 42-44 and 64-65 stand rejected under 35 USC 103(a) as being unpatentable over Candelore in view of Maillard et al (U.S. Patent No. 6,714,650). Claims 51-53 stand rejected under 35 USC 103(a) as being unpatentable over Candelore in view of Thompson et al (U.S. Patent No. 6,357,046). Independent claim 40 recites a conditional access method wherein particular data packets in a transport stream of successive data packets are detected, removed and encrypted and the encrypted data packets are inserted into the remaining base transport stream at "insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport system." In addition, claim 45 now recites that the encrypted data packets are "inserted at positions a predetermined number of data packets ahead of respective original positions." This is particularly important in terms of avoiding bottlenecks on the decryption side by providing time in advance of the normal data packet stream to decrypt a packet. By contrast, as pointed out by the Examiner, Candelore teaches that the selective encryption of data packets are made without modifying the order of the packets. Specifically, Candelore states in the last sentence of Paragraph [0089] as follows:

"Preferably, the [encrypted] packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same." (emphasis supplied)

The Examiner contends that Candelore clearly teaches placing the encrypted data packets in the data stream ahead of their original location, citing numerous paragraphs and Figures, none of which in applicant's view supports the Examiner's assertion. In particular, the Examiner refers to the statement in Paragraph [0037] that the "packets

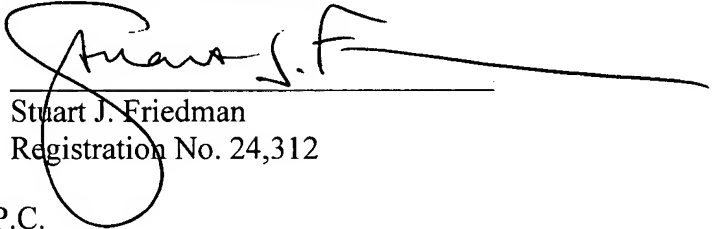
making up the encrypted pairs can occur in either order." However, a complete reading of Candelore reveals that the Examiner is picking and choosing convenient terminology without a careful consideration of what Candelore teaches as a whole. This language, in fact, appears to be actually referring to packets EA, based on legacy encryption, and packets EB, based on secondary encryption. These are the packets making up the "encrypted pairs" and which can be in either order EA then EB or EB then EA. See, paragraph [0056]. The language referred to by the Examiner has nothing whatever to do with selecting data packets for encryption and then inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport system to provide time for decryption. Indeed, Candelore does not teach or suggest, or even discuss, a solution to the problem of bottlenecking at the decryption side.

The Examiner fails to point to specific language in Candelore which expressly teaches the notion of placing the encrypted data packets in the data stream ahead of their original location. To the contrary this notion is specifically and expressly taught away from by Candelore. As a result, the advantages of the present invention, namely, that with low computation capabilities it is now possible, on the receiver side, to process an encrypted data packet and to reintroduce it at the right place in the data stream, is not attainable with Candelore. For this reason, Candelore cannot anticipate the subject matter of claim 1 and its dependent claims. As for Maillard et al and Thompson et al, it can be seen that these references also do not address this problem and certainly contain no teaching or suggestion to place the encrypted data packets in the data stream ahead of their original location. Indeed, as can be seen from paragraph 11 of the office action, Maillard et al was cited only for its disclosures regarding the event decryption key and regarding transmitting and recording digital data where the conditional access system includes a chip card with decryption circuitry. From paragraph 12 it can be seen that Thompson et al was cited only for its disclosure of a head-end encoder including a Common Interface CI as set forth in claims 51-53. There is no teaching in Maillard et al or Thompson et al which makes up for the deficiency in Candelore with respect to the

placement of encrypted data packets into the data stream. Accordingly, no combination of Candelore and Maillard et al or Candelore and Thompson et al can render the subject matter of claims 42-44, 51-53 or 64-65 unpatentable within the meaning of 35 USC 103(a).

In view of the foregoing, it is respectfully urged that claims 40-65 are now in condition for allowance and an early Notice of Allowance is courteously solicited.

Respectfully submitted,



Stuart J. Friedman
Registration No. 24,312

Law Offices of Stuart J. Friedman, P.C.
28930 Ridge Road
Mt. Airy, MD 21771
Telephone: (301) 829-1003
Facsimile: (301) 829-4107